Privacy Preserving Tools for Federated Authentication Models

NOTE: The Solicitations and topics listed on this site are copies from the various SBIR agency solicitations and are not necessarily the latest and most up-to-date. For this reason, you should use the agency link listed below which will take you directly to the appropriate agency server where you can read the official version of this solicitation and download the appropriate forms and rules.

The official link for this solicitation is: http://www.grants.gov/web/grants/view-opportunity.html?oppId=251550

Agency:
Department of Commerce

Release Date:
February 19, 2014
Branch:
n/a

Open Date:
February 19, 2014
Program / Phase / Year:
SBIR / Phase I / 2014

Application Due Date:
May 02, 2014

Solicitation:
2014-NIST-SBIR-01

Close Date:
May 02, 2014
Topic Number:
9.02.02.77-R

Description:

Legacy Internet communication protocols were designed for secure communication in the Dolev-Yao model. This model consists of two communicating parties and an adversary who can overhear, intercept, and synthesize any message. In this paradigm, the legitimate communicating parties only send messages to each other. No messages are sent to the third party, who is an adversary intent on preventing the legitimate parties from achieving its goal.

In the last few decades, software and standards have been developed which satisfactorily solve the above problem. Current digital transactions, however, occur in a model that is very different from Dolev-Yao. Specifically, third parties are not necessarily malicious and, in fact, often are an important part of a multi-party communication protocol. These protocols seek to enhance the digital world. In particular, they aim at facilitating electronic commerce and other transactions in a cooperative, rather than adversarial, model. Of course, we cannot simply assume bad actors away. The next generation of protocols needs to replace “distrust” by “trust but verify.” It seeks to use novel Internet technologies (see, for example, the NIST Beacon at http://www.nist.gov/itl/csd/ct/nist_beacon.cfm).

In the modern internet world, with its myriad players - customers, standards bodies, industry, governments, privacy advocates, and many more - it will be hard to effect this transition. But transition we must if we are to realize the potential of the Internet for improving our quality of life

and, from the United States perspective, our competitiveness.

However, industry and other actors often resist modification to its deployed technologies. This subtopic is about overcoming this critical barrier by focusing on test cases that are representative of many scenarios and specific enough to allow engineering of working solutions. So as to maximize the probability of successful commercialization and adoption by industry, these solutions should leverage existing Dolev-Yao protocols and standards by either using them as black-box primitives or implementing minimal changes to them.

A primary objective is to develop tools that solve remote authentication, identification, and attribute disclosure problems (e.g., JSON, SAML, OpenID Connect, OAuth). A representative problem is the "brokered identity problem," in which there are identity and attribute providers that, due to privacy considerations, must issue assertions without knowing who the consumer of the assertion is. For example, an attribute verifier does not need to know what application the user is attempting to access. Signed assertions are issued and sent to a broker, who in turn forwards them to the assertion consumer, typically a service provider. It is fairly straightforward to use two-party protocols such as SAML to solve this problem if we are willing to allow the broker to read the assertions. However, it is more complicated to solve this problem under the so-called "honest but curious model" in which the broker follows the protocols but anything that it learns becomes public knowledge. The recipient will specifically develop and test working technologies that solve attribute disclosure problems in a multi-party authentication architecture for privacy preserving protocols outside the Dolev-Yao model.

Phase I activities and expected results:
Pick one or more representative problems;

1. Research solutions from the cryptographic literature; and/or
2. Choose candidate techniques and carry a preliminary assessment of how these choices impact feasibility vis-à-vis compatibility with existing standards and industry practice.

Phase II activities and expected results:
Develop working prototypes and work with NIST, the NSTIC NPO [1], and industry to carry out feasibility tests and evaluations, with an eye toward downstream commercialization.

On a case-by-case basis, NIST may provide technical experts to work with Phase I and Phase II awardees for consultations and discussions to answer design questions and clarify any other technical aspects within the field of expertise.